Robust Watermarking Approach Based on Coefficient Comparison of Detail Sub-bands of DWT

Qiudong Sun, Yufeng Shao, Liandong Wang, Lin Gui and Wenying Yan

School of Electronic and Electrical Engineering　　Shanghai Second Polytechnic University, Shanghai 201209, China
{qdsun, yfshao, ldwang, guilin & wyyan}@sspu.edu.cn

Abstract - This paper presented a novel watermarking method to protect copyrights for digital media. Firstly, a visual model is employed to calculate the block based just noticeable difference (JND) to control the embedding intensity to improve the transparency and robustness of watermarking. Then, two neighboring image blocks are selected each time in Hilbert scanning order, and transformed by discrete wavelet transform (DWT) respectively. Lastly, according to the JND and the watermark bit, the values of two corresponding detail sub-bands coefficients in DWT domain is adjusted to embed the watermark. In this algorithm, a couple of coefficients in two corresponding detail sub-bands can embed a bit of watermark sequence. This embedding method guarantees hiding enough copies of watermark into the host image and improves its performance. The experimental results show that the embedded watermark is invisible, and the algorithm is robust to general image processing operations. The conclusion is that the algorithm is effective and practical.

Index Terms - Robust watermarking; Just noticeable difference; Discrete wavelet transform; Detail sub-band; Coefficient adjustment.

1. Introduction

Along with the development of information technology, people have paid more and more attention on the information security today. The technique of digital watermarking in an image has become a research focus for information security and copyright protection. For an effective digital watermarking scheme, three basic requirements should be satisfied: transparency, robustness and security. The former two are in conflict with each other. To dissolve this conflict availably, we can consider using the masking characteristic of human visual system (HVS) [1]. Generally, the digital watermarking methods are classified into two types. One works in spatial domain, and the other in the transform domain, such as DWT or DCT. Generally, the latter is more desirable because the energy of embedded data in transform domain is spread over all areas of image in the spatial domain. Duo to its good time-frequency localization function is similar to the visual masking of HVS, the DWT has been used widely in the field of watermarking [2]. A good watermarking technique also should extract the watermark bits from embedded image blindly.

In recent years, many algorithms based on HVS and DWT had been proposed for watermarking [1-9]. But there is no one considering the comparability of corresponding DWT detail sub-bands of two neighboring blocks of image and embedding watermark in them according to their feature adjustment.

In this paper, we propose a robust watermarking method based on coefficient relations in DWT domain and visual model, which supports embedding a small binary image as watermark. As mentioned previously, in order to adjust the input image for transparent watermarks, we employ a visual perception model [2, 4, 10] to calculate the different JND (just noticeable difference) thresholds for determining the intensity of watermarking at the different locations of image. We also give a redundant encoding method for robustness.

This paper is organized as follows. In section II, we introduce a visual perceptual model and give a JND thresholds calculation equation for controlling the embedding intensity. Section III presents the watermarking algorithm and its extraction in detail. Section IV examines the performance of proposed algorithm, and shows that the proposed method achieves more effective and better performance, both in terms of transparency and robustness through simulation. Section V gives the conclusion of this paper.

2. Visual Perceptual Model and JND Calculation

A. Visual Perceptual Model

Under the background gray f, the human eyes relative sensitivity to gray change $\gamma(f)=\Delta f/f$, which is a non-linear function of f, can be approximated by the equation as follows [10]:

$$\gamma(f) = \frac{\Delta f}{f} = 0.02\left[e^{\frac{128}{f}-1} + e^{\frac{1}{(256-f)}-\frac{1}{128}} \right], \qquad (1)$$

where e is the base of natural logarithm. In experiment, we can use the gray mean of $K \times K$ image block $\boldsymbol{B}_{uv}$ located at (u, v) as the background gray, i.e. f=mean($\boldsymbol{B}_{uv}$).

B. JND Calculation

To ensure that the watermark has good transparency and robustness, we can use JND to adjust the intensity of watermark-embedding [2,4]. The image block $\boldsymbol{B}_{uv}$ is DWT-transformed into a approximate image and three detail sub-band images $\boldsymbol{D}_{uv}^{s}$ ($s \in$ HH,HL,LH, represent the three detail sub-bands of diagonal, horizontal and vertical directions respectively). The JNDs of three detail sub-bands are represented as follows:

$$\boldsymbol{J}_{uv}^{s} = \boldsymbol{T}_{uv}\boldsymbol{F}_{s}, \qquad (2)$$

where $\boldsymbol{T}_{uv}$ is the normalized value of $\boldsymbol{T}_{uv}' = f\gamma(f)\boldsymbol{E}_{uv}$ at the range $[a, b]$, while $\boldsymbol{E}_{uv}$ is the normalized entropy of $\boldsymbol{B}_{uv}$. When $s \in$ HH, $\boldsymbol{F}_{s}$ equals $\sqrt{2}$, otherwise it is 1 [4].

3. Watermarking Algorithm

A. Watermark Embedding

Let W represents a watermark sequence, B_{uv1} and B_{uv2} are the two neighboring image blocks and their DWT-transformed detail sub-bands are D_{uv1}^s and D_{uv2}^s (simply marked by D_1 and D_2, or by a universal symbol D_t, $t \in \{1, 2\}$). Now we can define the admissible distortion factor of sub-band coefficients of DWT as follows:

$$\lambda_t = \frac{|D_t| + \delta}{\text{mean}(|D_t|) + \delta} \qquad t \in \{1, 2\}, \qquad (3)$$

where δ is a positive number, which is a effect factor of absolute values of detail sub-band coefficients to embedding intensity. When the block size is 2×2, whatever the size of δ is, the equation (3) is constant and can be simplified to $\lambda_t = 1$.

We also assume that μ is the mean value of JNDs of two neighboring blocks, Δd is their corresponding DWT detail sub-band coefficients difference at same direction, and ε is the adjustment intensity matrix of detail sub-bands coefficients. They are represented by equations as follows respectively:

$$\mu = \frac{1}{2}\left(J_{uv1}^s + J_{uv2}^s\right), \qquad (4)$$

$$\Delta d(i, j) = \text{Sign}\left(W_k\right)\left[D_2(i, j) - D_1(i, j)\right] , \qquad (5)$$

$$\varepsilon_t(i, j) = \frac{1}{2}\text{Sign}\left(W_k + t\right)\lambda_t(i, j)\left[\mu - \Delta d(i, j)\right], \qquad (6)$$

where Sign($\cdot$) is a sign function, it is defined as follows:

$$\text{Sign}(x) = \begin{cases} 1 & x \in \text{even} \\ -1 & x \in \text{odd} \end{cases},$$

W_k is the k-th element of binary watermark sequence W. We can prove that the watermark embedding rule is as follows:

$$D_t'(i, j) = \begin{cases} D_t(i, j) + \varepsilon_t(i, j) & \text{if } \Delta d(i, j) < \mu \\ D_t(i, j) & \text{otherwise} \end{cases}. \qquad (7)$$

From the embedding rule, we know that a couple of coefficients in the two corresponding detail sub-bands can embed a bit of watermark. So, if the size of host image is $M \times N$, the embedding capacity of this algorithm can reach to the value of $(3MN)/8$ bits. For example, if the size of host image is 512×512, then the full embedding capacity is 98304 bits or 12288 bytes. It is large enough to embed watermark into a host image. So, this method can bring an enough redundancy to ensure the watermark's robustness.

B. Watermark Extraction

Being the same with watermark embedding, the blind extraction rule can be proved as follows:

$$\hat{W}_k(i, j) = \begin{cases} 1, & \text{if } \hat{D}_2(i, j) \leq \hat{D}_1(i, j) \\ 0, & \text{otherwise} \end{cases}, \qquad (8)$$

where $\hat{D}_t$ is the DWT detail sub-bands of embedded image block, $\hat{W}$ is the watermark bit sequence extracted from embedded image block.

C. Embedding Algorithm

1) A binary watermark image will be converted into a bit stream W. It's called the original watermark.

2) In order to enable that the length of original watermark W is just equal to 24 times of total blocks number of host image, some zeros can be appended to the end of it.

3) For improving the robustness of watermarking, the redundancy of embedded watermarks should be ensured. So the original watermark W should be extended periodically as follows:

$$W_{\text{ex}}^m = W_l \quad m = n \cdot L + l; n = 0, 1, \cdots, Cr - 1; l = 0, 1, \cdots, L - 1, \quad (9)$$

where W_{ex} is the extended watermark, W_{ex}^m represents its m-th element, Cr is the extended factor.

4) For improving the security of watermarking, W_{ex} should be scrambled randomly.

5) In order to keep the relativity of two neighboring image blocks, we can scan the original host image by Hilbert scanning to obtain a Hilbert scanning sequence.

6) The two neighboring image blocks B_{uv1} and B_{uv2} are selected each time from the host image with Hilbert scanning order, and embedded the watermark according to the method as mentioned above in this section until all DWT detail sub-bands of all blocks have been processed.

7) After applied the inverse DWT for all watermark embedded blocks, we can get an embedded image I'.

D. Extracting Algorithm

1) Scan the embedded image I' by Hilbert scanning with the same order as that in embedding.

2) Two neighboring image block B'_{uv1} and B'_{uv2} are selected each time from the embedded image with Hilbert scanning order, and extracted the watermark according to the method as mentioned above in this section until all blocks have been processed.

3) Now we can get a watermark sequence $\hat{W}_{\text{ex}}$, which involves the Cr copies of original watermark.

4) If there was a scrambling when watermark was embedded, here we should do unscrambling to $\hat{W}_{\text{ex}}$.

5) The final watermark can be obtained from $\hat{W}_{\text{ex}}$ as follows:

$$\hat{W}_l = \begin{cases} 1, & \text{if } \sum_{n=0}^{Cr-1} \hat{W}_{\text{ex}}^{n \cdot L + l} \geq \frac{Cr}{2} \\ 0, & \text{else} \end{cases}. \qquad (10)$$

6) The binary watermark sequence $\hat{W}$ should be converted back into a binary image.

4. Experiment Results and Performance Analysis

The peak signal to noise ratio (PSNR) is employed to evaluate the quality of embedded image, meanwhile the

normalized correlation coefficient (ρ) between the extracted watermark and the original one is employed to evaluate the quality of watermarking technique.

A. Impact of Parameters on Algorithm

In the experiment, the proposed algorithm is evaluated on the gray image "Lena" (512×512). The block size K can be 8, 4 or 2. Fig. 1 is the relationship between PSNRs of embedded image and the effect factor δ at different block size. Fig. 2 is the relationship between PSNRs and the JND normalized range $[a, b]$ at full capacity embedding. Fig. 3 is the relationship between BER of the recovered secret bits and the JND normalized range $[a, b]$.
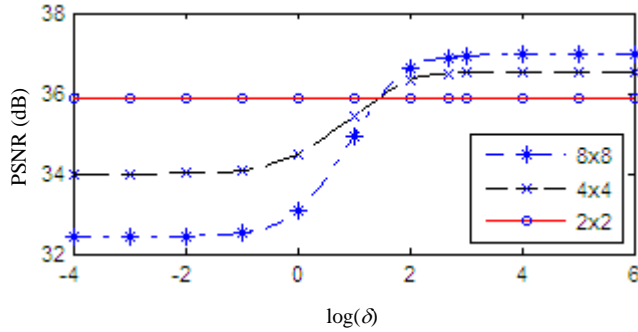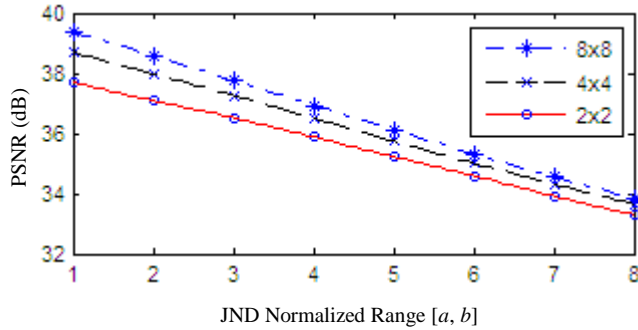

Fig. 1 Relationship between PSNR and δ.

Fig. 2 Relationship between PSNR and $[a, b]$ ($b=a+1$).

As shown in Fig.1, the PSNRs of embedded image at different δ are constant when $K =2$, but when $K >2$, the bigger δ is, the higher PSNRs are. When δ=31.65, the PSNRs of embedded image are almost same whatever K is. When δ<31.65 and K=8 or K=4, the PSNRs of embedded image are lower than that of K=2. When δ>31.65 and K=8 or K=4, the PSNRs of embedded image are higher than that of K=2. When δ=1000, the PSNRs almost reach their maximums respectively and tend to constancy. So we set the δ=1000 in the following experiments. As shown in Fig. 2, the PSNRs are almost in inverse proportion to $[a, b]$. The smaller $[a, b]$ is, the higher PSNRs are, and the better imperceptibility of embedded watermark is. But as known in section II, the smaller $[a, b]$ will bring down on the embedding intensity, it leads that the performance of extracting algorithm becomes worse. So that an appropriate $[a, b]$ is better. Here, we set $[a, b]$=[4, 5].

B. Watermarking Results

Figs. 3(a) and 3(d) are the original images of "Lena" and "Elaine" respectively. Figs. 3(b) and 3(e) are their embedded results when K=8, and their PSNRs are 36.9dB and 36.6dB respectively. Figs. 3(c) and 3(f) are their differences between the original images and embedded images at the condition of magnifying 30 times. As shown in Fig. 3, due to considering the visual perception in the algorithm, the embedded watermark in different host images is invisible. The algorithm can also fully extract the embedded watermark from the embedded image.
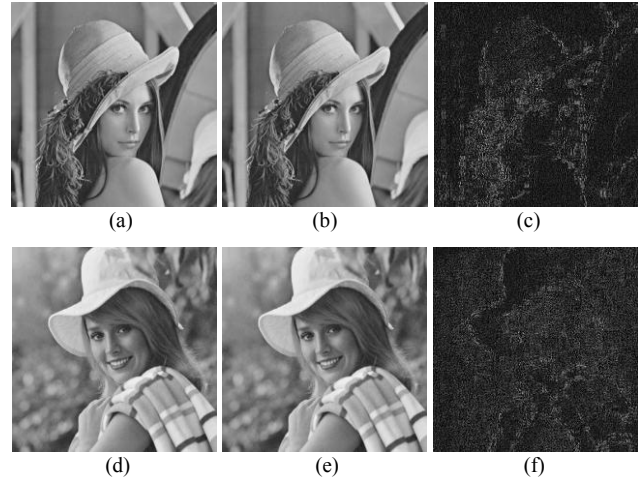

Fig. 3 Watermark embedded results of "Lena" and "Elaine".

C. Performance Variety on Various Attacks

In the experiment, all attack items are operated on Photoshop CS, besides the JPEG compression and central region cropping. Fig. 5 is the binary image watermarking results of the proposed algorithm acting on the gray image "Lena". Fig. 5(a) is the original binary watermark image (32×32). Fig. 5(b)~(h) are the recovered copies from the watermarked image by attack of cropping the central region with size 300×300, zooming out to size 450×450 and zooming in, JPEG compression with 90% quality, adding Gaussian noise with 10%, eddy distortion with 100% degree, contrast enhancement with 70% and 10 times edge enhancement respectively. As shown in Fig. 5, the watermarking algorithm is robust against the general image processing methods.

Fig. 4 Watermarking results of a binary image.

D. Performance Comparison of Different Block Sizes

In the experiment, we also give the normalized correlation tests of various attack defenses of watermarking and its performance comparison of different block sizes. As shown in Table I, the robustness of watermarking is good whatever the

block size is selected, and their performances just have slight differences.

TABLE I   Robustness of Watermarking Against Different Image Processing Methods

Attack items	The Normalized Correlation Coefficient ρ		
	8×8	4×4	2×2
Brightness enhancement (100%)	1	1	1
Contrast enhancement (70%)	1	1	1
Edge enhancement (10times)	1	1	1
Histogram equalization	1	1	1
Extrusion distortion (100%)	0.9840	0.9741	0.9859
Eddy distortion (100%)	0.9962	0.9766	0.9933
Add Gaussian noise (10%)	0.8828	0.8925	0.9102
Add uniformity noise (10%)	0.9836	0.9819	0.9830
Add salt & pepper noise (10%)	1	1	1
Cropping in central region (300×300)	0.9981	1	1
Zoom out and Zoom in (450×450)	0.9744	0.9952	1
JPEG compression (90% quality)	0.9952	0.9962	0.9914

4. Conclusions

This paper presented a novel method of watermarking in gray images based on DWT. In our approach, the comparability of corresponding DWT detail sub-bands of two neighboring image blocks was considered, and in order to improve the invisibility of watermark, the visual model was also used for determining the embedding intensity at different locations. In addition, in order to defense the general image processing attacks, the redundant encoding was given for increasing the embedded copies of watermark. The experiment results demonstrated that the proposed algorithm yields the acceptable performance for transparency and robustness to general image attacks.

References

[1] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 783-791, May 2001.

[2] H. F. Yang, X. W. Chen, "A robust image-adaptive public watermarking technique in wavelet domain," *Journal of Software*, vol. 14, 1652~1660, September, 2003.

[3] J. G. Cao, J. E. Fowler, and N. H. Younan, "An image-adaptive watermark based on a redundant wavelet transform," *IEEE International Conference on Image Processing*, vol. 2, pp. 277-281, 2001.

[4] Z. M. Wang, Y. J. Zhang, and J. H. Wu, "A wavelet domain watermarking technique based on human visual system," *Journal of Nanchang University (Natural Science)*, vol. 29, pp. 400~403, April, 2005.

[5] D. Y. Liu, and W. B. Liu, "Adaptive SVD-based wavelet domain watermarking scheme for color image authentication," *Computer Engineering and Application*, vol. 43, no.36, pp. 107–109, December, 2007.

[6] L. Y. Wu, and F. Yang, "An improved digital watermarking algorithm based on DWT," *Control and Automation*, vol. 23, no. 6-3, pp. 46–47, 59, June, 2007.

[7] M. R. Huang, B. J. Gao, and Y. J. Han, "CDMA adaptive watermarking algorithm based on wavelet basis," *Computer Engineering*, vol. 34, no.23, pp. 184–186, December, 2008.

[8] X. L. Zhu, and J. S. Zhang, "Adaptive digital watermakring algorithm based on energy analysis of wavelet cofficients block," *Journal of Computer Applications*, vol. 26, no. 4, pp. 830-832, April, 2006.

[9] F. K. Yang , Q. M. Zheng, and X. H. Jiang, "A watermarking algorithm based on block energy analysis of the wavelet tranform parameters and chaotic map," *Microcomputer Applications*, vol. 29, no. 2, pp. 32-35, February, 2008.

[10] Q. D. Sun, "An adaptive algorithm for edge detection based on visual perception model," *Journal of Shanghai Second Polytechnic University*, vol. 15, no. 2, pp. 83~90, October, 1998.